You don’t have to work in the finance department of a big company to be the target of business email scams. Business Email Compromise (BEC) is the FBI’s term for financial attacks where the target is contacted through their work email. The attacker uses a hacked or fake account that looks like the real thing in an effort to con the target.

How to Protect Yourself

**Be proactive:**

- **Know your company’s cyber security plan** and how to respond to any suspicious emails.

- **Confirm all unusual money requests** in person or on the phone. If an email looks strange, look up the sender and call them (don’t use the number they provide).

- **Invest in antivirus software** and other cyber security software that can flag suspicious emails and websites.

- **Never trust unknown individuals.** Verify everything they claim and do not send sensitive information to anyone whose identity you can’t confirm.

- **Don’t reply to emails from people you don’t know** or click on their links or attachments. Cyber criminals could be trying to gain access to your company network.

- **Wait, if you are at all unsure.** Take the time to discuss your suspicions with your manager or a colleague.

**If you suspect you’ve been targeted:**

- **Don’t delay.** Acting quickly after an attack can minimize damage to your business.

- **Call your bank** and freeze financial accounts that may be affected (Bank of America’s number for stolen or lost cards is 800-432-1000), inform credit bureaus and change passwords that may have been breached.

- **Call the police** and file reports with the relevant local authorities.

- **Document everything** about the attack. The more information you have, the better armed you will be to assist an investigation by your company, your bank and law enforcement officials, and the better prepared you will be against future attacks.

---

Why It’s Important

Cyber criminals are casting their nets wide, with targets ranging from wealthy individuals, families and beyond to employees at small businesses, nonprofits, school systems and churches. A common attack is called phishing, where bogus messages are sent via email or messaging platforms. Phishing is a threat for business, as well as personal, email accounts.

- **Vishing** is the phone version of phishing, and **smishing** is the SMS or messaging app version.
- **Spear phishing** involves targeting high-profile individuals.
- **Spoofing** is when criminals pretend to be someone else, or a legitimate business, to get your personal information.

Cyber criminals go phishing by:

1. **Contacting you** through spoofed or compromised email accounts or accounts for messaging apps like Instagram and Facebook
2. **Offering a “bait”** that gets you to click a link, which downloads spyware to your computer and gives criminals access to your device and information
3. **Providing an urgent pretext** for why you must send confidential or financial information

Other business email scams can come from:

- **A supplier.** Arrives from a hacked email address to notify you of a bank account change or to request payment.
- **An attorney.** Often arrives during a transaction such as a home purchase, with directions to send an expected payment, like a down payment.
- **A familiar address.** Appears to come from someone you know and asks for confidential information, like payroll records.

**IMPORTANT INFORMATION**

Neither Bank of America nor its affiliates provide information security or information technology (IT) consulting services. This material is provided “as is,” with no guarantee of completeness, accuracy, timeliness or of the results obtained from the use of this material, and without warranty of any kind, express or implied, including, but not limited to warranties of performance, quality and fitness for a particular purpose. This material should be regarded as general information on information security and IT considerations and is not intended to provide specific information security or IT advice nor is it any substitute for your own independent investigations. If you have questions regarding your particular IT system or information security concerns, please contact your IT or information security advisor.

Merrill Lynch, Pierce, Fenner & Smith Incorporated (also referred to as “MLPF&S” or “Merrill”) makes available certain investment products sponsored, managed, distributed or provided by companies that are affiliates of Bank of America Corporation (“BofA Corp.”). MLPF&S is a registered broker-dealer, Member SIPC, and a wholly-owned subsidiary of BofA Corp.

Bank of America Private Bank is a division of Bank of America, N.A., Member FDIC, and a wholly-owned subsidiary of BofA Corp.

Banking products are provided by Bank of America, N.A., and affiliated banks, Members FDIC, and wholly-owned subsidiaries of BofA Corp.

Investment products:

<table>
<thead>
<tr>
<th>Are Not FDIC Insured</th>
<th>Are Not Bank Guarenteed</th>
<th>May Lose Value</th>
</tr>
</thead>
</table>

© 2019 Bank of America Corporation. All rights reserved.